

SECURITY FEATURES OF BEL'S ELECTRONIC VOTING SYSTEMS

Process security and reliability are paramount in a voting system. In order to maintain the integrity of the process, a combination of technological innovations have been very successfully integrated into the machines made by BEL

Bharat Electronics Limited (BEL), a Public Sector Enterprise of the Government of India and a multi-product Electronics company, manufactures Electronic Voting Machines, (EVMs) which are being regularly used in the elections of largest democracy of the world – INDIA where approximately 671 million voters cast their votes.

be custom made to suit any electoral process, like Single Election, Multiple Election (Two simultaneous elections), Multiple Selection (more than one party & candidate), Proportional Representation etc,. These machines not only save time, but also are cost-effective and more importantly tamper-resistant.

SECURITY FEATURES OF BEL'S ELECTRONIC VOTING SYSTEMS

Process security and reliability are paramount in a voting system. In order to maintain the integrity of the process, a combination of technological innovations have been very successfully integrated into the machines made by BEL

Exclusive use of EVM's across the length and breadth of a huge country like India has come off splendidly and the unparalleled success of this bold and progressive process demonstrated to the rest of the world, the country's technological capabilities. About half a million of the EVM's deployed in these elections were designed, manufactured and delivered by BEL. Today, BEL is one of the largest and successful manufacturers of EVM's worldwide.

The pattern of electoral process varies from country to country. Recognising this variation and the need to address it, a dedicated in-house R&D group of BEL has competently customized and upgraded the product for the successful use in the global market. Electronic Voting Systems can

Process security and reliability are paramount in a voting system. In order to maintain the integrity of the process, a combination of technological innovations have been very successfully integrated into the machines made by BEL, which are detailed below:

**Irreversible polling process
implemented
in the functioning of the
machine**

**Hardware
Mechanism**

Protection

The Control unit contains a Micro-controller Integrated Circuit with the main program codes permanently fused into the device, which is

manufactured as a proprietary item for BEL and a Non Volatile Memory that stores the polled data. These two devices are most critical in the voting chain and protected against tampering by the following methods:

- Unique serial numbers are captured on the printed Circuit Board (PCB) and its records are maintained at the factory.

OTP Micro-controller and Non-volatile memory and its proprietary protocol

- Manufacturer's ID number is provided, for BEL's proprietary Micro-controller and the records are maintained at the factory.
- Micro-controller IC and Non-Volatile Memory IC are assembled onto the PCB by a special soldering process at the factory. Any tampering / replacement of these devices, leave a residue and can be easily identified with a visual look at the solder joint by experts.

Firmware Protection Mechanism– One Time Programmable Device (OTP):

Following are the Firmware protection mechanisms are incorporated in the micro controller IC, in order to prevent alteration / modification to the program code and the polled data:

in this OTPROM permanently. Program codes once written and fused in this OTPROM cannot be **read back** or altered by anyone including the manufacturer. Thus, it is 100% code protected from either altering or decoding the contents.

- The Program code residing in the Micro-controller OTPROM does not accept data from any other external device other than BEL made Ballot Unit, which is part of the voting system, and thus an integrity check is built-in.
- Address and Data lines of the OTP Micro-controller are not accessible from outside.
- EVM is a stand-alone system and does not have any operating system and connectivity with Internet, and hence not vulnerable to hacking.

Non-Volatile Memory:

The memory device used in the EVM does not require a battery backup and can store the polled data adequately. It can be written only through the command signal from the Micro controller under specific conditions controlled by the program code.

Hence, the Non-Volatile Memory and Micro Controller are tightly integrated.

Following are the Protection / Tamper resistance features of the Memory:

Multi level locks and thread sealing in control unit and balloting unit

- Micro-controller has a One Time Programmable Read Only Memory (OTPROM). Program codes are fused

- Polled data is encrypted and stored in the memory, which makes it inaccessible.
- Memory and OTP Micro-Controller have tightly coupled handshake protocol and matched. The code residing inside the Micro Controller verifies the encrypted data pattern stored in the Memory for integrity check and to ensure it is the right type of memory and then only it establishes transfer of data to and from the memory. Any tampering of the memory device or altering the data in the memory will result in machine Error status, and will appear on the display of the Control unit.

Tamper evident sticker in control unit

Other Factors:

Ballot Unit is integrated with the Control unit through a signal integrity method. The program code stored with Micro-controller device checks for the presence of a specific Balloting Unit (i.e. BEL made only) before establishing data communication. Control Unit will not accept data from any other Balloting Unit device other than that of BEL make because of the proprietary integrity check method.

The Electronic Voting Machine (EVM) works in an irreversible cycle of polling process in which the following features are incorporated:

- No voting is possible without interconnecting the preset Balloting Unit.

- Not possible to change the number of contesting candidates in a given polling process.
- Polled data cannot be cleared till the result is seen.
- No voting is possible after the closing of poll.

To summarise, the Electronic Voting Systems from BEL offers a very high degree of tamper resistance through the following features:

- Irreversible polling process implemented in the functioning of the machine
- Multi level locks and thread sealing in control unit and balloting unit
- Tamper evident sticker in control unit
- OTP Micro-controller and Non-volatile memory and its proprietary protocol
- Being a stand-alone system, hacking is impossible

Being a stand-alone system, hacking is impossible.

election process, nullify the errors, prevent tampering/ hacking and also make it cost effective. All these aspects have been appropriately taken into account with priority accorded to security, thus assuring a clean election.

